瑞星 **EXCHANGE** 邮件病毒监控系统使用手册

北京瑞星科技股份有限公司

目 录

第一章 简介

随着因特网的飞速发展和迅猛普及，电子邮件系统已经成为现代企业和广大用户进行通信与信息交流的主要手段。比较常用的电子邮件系统有 Microsoft Exchange 和 Lotus Domino 等，这些系统在方便信息交流的同时，也为病毒提供了一个感染和快速传播的捷径。这就给防病毒厂家提出了新的挑战，要求能够对邮件系统进行病毒防护。瑞星 Exchange 邮件病毒监控系统就是这样一个产品。

Microsoft Exchange 是微软出品的电子邮件和协作系统，它通过电子邮件来交换信息，实现工作组成员间的相互协作。Microsoft Exchange 支持 SMTP、POP3、IMAP4 等多种协议，是被众多国内企业采用的一种流行的电子邮件系统。瑞星 Exchange 邮件监控系统为这些企业提供了全面的、完善的针对 Microsoft Exchange 邮件系统的防病毒解决方案。

瑞星 Exchange 邮件监控系统的主要功能特色包括：

（1） 自适应 Microsoft Exchange 的不同版本：瑞星 EXCHANGE 邮件病毒监控系统支持 Exchange 5.5 和 Exchange 2000，安装程序能够自动识别 Exchange Server 的版本，安装合适的文件。

（2） 实时防护：能够对邮件附件进行实时扫描，对带毒邮件做到立即发现、立即清除、立即报警。对于 Exchange 5.5，采用 MAPI 方式的实时监控，对新到的邮件进行实时扫描。对于 Exchange 2000，支持双层实时监控：MAPI 实时监控和 SMTP 实时监控，监控范围更全面。

（3） 自动报警：发现病毒后，支持多种通知用户的方式：Windows NT EventLog ，记录病毒日志文件，给相关人员发送病毒警告邮件（包括发件人、收件人、指定的管理员）、在邮件中插入病毒警告信息附件。

（4） 手动扫描：瑞星 Exchange 邮件病毒监控系统提供了功能强大的手动扫描程序，使得管理员能够随时对所有用户邮箱和公用文件夹中的邮件进行扫描，使病毒无处藏身。

（5） 自动升级：瑞星 Exchange 邮件病毒监控系统能够定期自动升级，对病毒定义文件和程序文件进行更新，保证了对携带最新病毒的邮件的查杀，使病毒无法逃脱。

第二章 安装和卸载

一、安装前的准备工作

1. Exchange5.5 邮件服务器上的安装

1) 如果已经安装了瑞星 EXCHANGE 邮件病毒监控系统的旧版本，请先卸载。为

了确保正确安装新版本的瑞星 EXCHANGE 邮件病毒监控系统，请在卸载完成后注销当前用户。

2) 以 Exchange Server Service Admin 帐号（Microsoft Exchange Server Service 使用的管理员帐号）登录 Windows NT/2000。

3) 瑞星 Exchange 邮件病毒监控系统安装程序并不检查用户输入的帐号是否为 Exchange Server Service Admin 帐号，如果输入不正确，将导致 Rising ScanExchange Service 不能启动，因此在输入前请确认帐号是否正确。如果您不清楚 Exchange Server Service Admin 帐号，请向管理员查询。

2. Exchange2000 邮件服务器上的安装

1) 如果已经安装了瑞星 EXCHANGE 邮件病毒监控系统的旧版本，请先卸载。为了确保正确安装新版本的瑞星 EXCHANGE 邮件病毒监控系统，请在卸载完成后注销当前用户。

2) 由于在 Exchange 2000 上没有 Exchange Server Service Admin 帐号，在安装瑞星 Exchange 邮件病毒监控系统之前，必须存在这样一个帐号：该帐号是 Exchange Administrator，并且在“Domain control Policy”（域控制器）级别上具有“以操作系统方式操作（Act as part of the operating system）”和“作为服务登录（Log on as a service）”的权限（如图 2-1），而且该帐号拥有邮箱（通常安装 Microsoft Exchange Server 时所用的帐号，再赋予以上两个权限之后就是合乎条件的帐号）。为了使修改的权限生效，设置完后重启机器，并使用此帐号登录 Windows NT/2000。

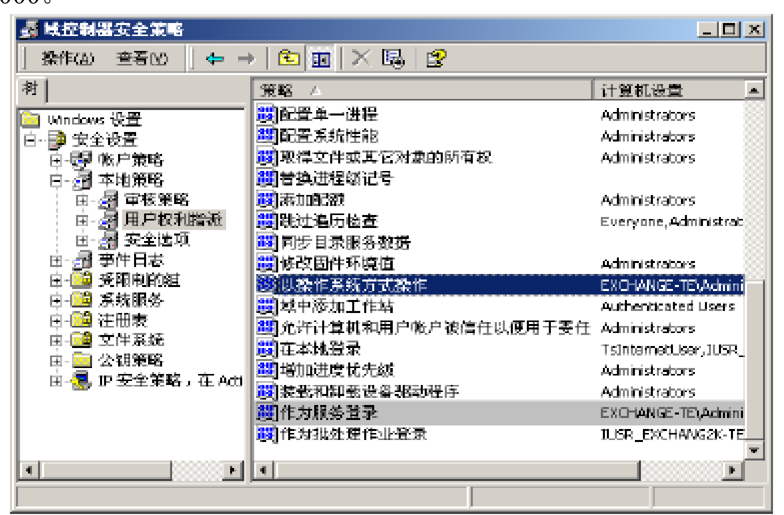


图 2-1

3) 瑞星 Exchange 邮件病毒监控系统安装程序并不检查用户输入的帐号是否为满足（2）中条件的帐号，如果输入不正确，将导致 Rising ScanExchange Service 不能正常启动，因此在输入前请确认帐号是否正确。

二、安装步骤

1. 运行瑞星 EXCHANGE 邮件病毒监控系统安装程序，运行后如图 2-2。



图 2-2

2. 单击按钮“下一步”，安装程序提示你将要安装瑞星 EXCHANGE 邮件病毒监控系统,以及提示版权所有。

3. 单击下一步，输入姓名、公司名称以及产品序列号，如图 2-3。



图 2-3

4. 单击下一步，输入 Exchange Server Service Admin 帐号、口令和域名称，如图 2-4。

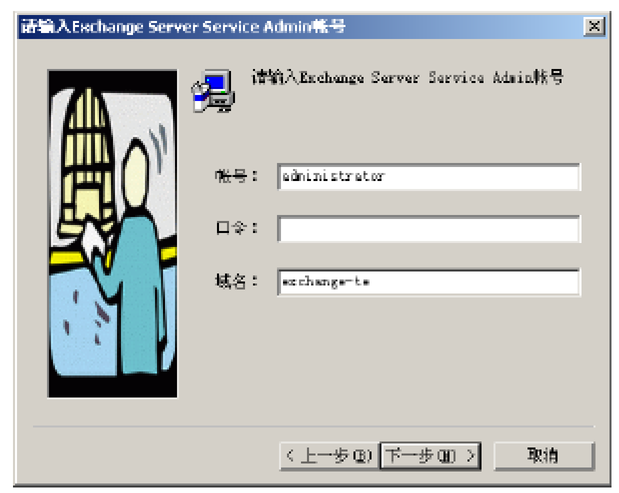


图 2-4

5. 单击下一步，选择软件安装目录，如图 2-5。

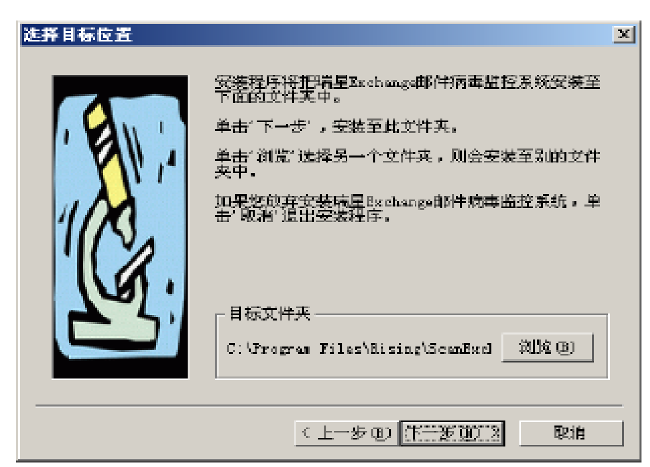


图 2-5

6. 单击下一步，确定安装的 EXCHANGE 版本和安装目录。

7. 单击下一步，开始安装文件，在此过程中，系统会停掉一些服务，并在安装完成后重启那些被停止的服务，如图 2-6 和图 2-7。（说明：图 2.6 和 2.7 中停止/重启有关服务的界面只有在 Exchange 2000 邮件服务器中才会出现，在 Exchange 5.5 邮件服务器中安装时不会出现图 2.6 和图 2.7 的界面。）



图 2-6

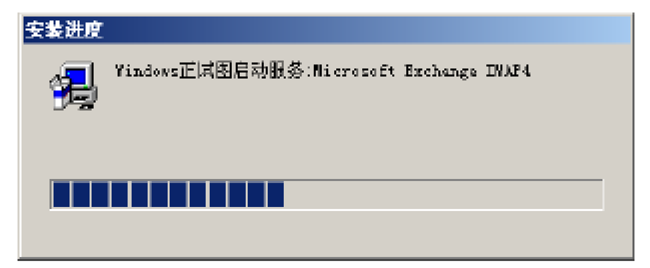


图 2-7

8. 装完成后，提示安装完成，单击按钮“完成”结束安装，如图 2-8。

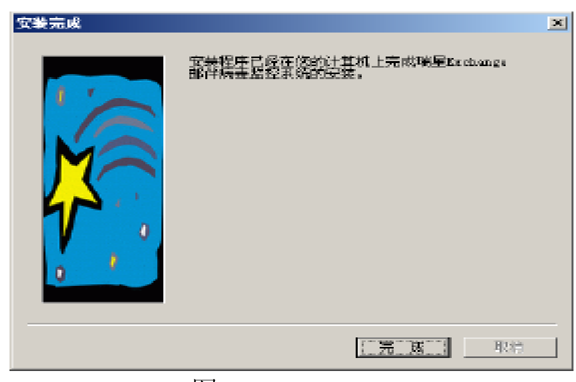


图 2-8

➢ 注意事项

✧ 瑞星强烈建议您不要将 Exchange Server 安装在 Windows NT 4.0，Terminal Server Edition 和 Windows 2000，Terminal Service（即安装了 Terminal Service 可选组件的 Windows 2000）这样的操作系统中，瑞星 Exchange 邮件病毒监控系统有可能无法正常工作在 Terminal Server 环境中。如果您确实需要在上述操作系统中安装 Exchange Server，请使用“安装模式”来安装瑞星 Exchange 邮件病毒监控系统（在安装前切换到安装模式：在命令提示符下运行 change user /install。安装完成后切换回正常的运行模式：change user /execute）。

✧ 在 Exchange 2000 服务器上的安装，一定要预先设置好要使用的帐号的权限。

三、卸载

瑞星 Exchange 邮件病毒监控系统提供了自动卸载的功能，使您可以方便的卸载瑞星 Exchange 邮件病毒监控系统的文件、程序组、快捷方式等。直接单击程序组“瑞星 Exchange 邮件监控”中的“卸载 Exchange 邮件监控”菜单，单击“卸载”按钮，程序自动完成卸载工作。

第三章 功能

一、MAPI 实时监控设置

如图 3-1 所示，MAPI 实时监控设置中包含两部分：启动 EXCHANGE 的 MAPI 邮件监控设置和发现病毒后的通知设置。

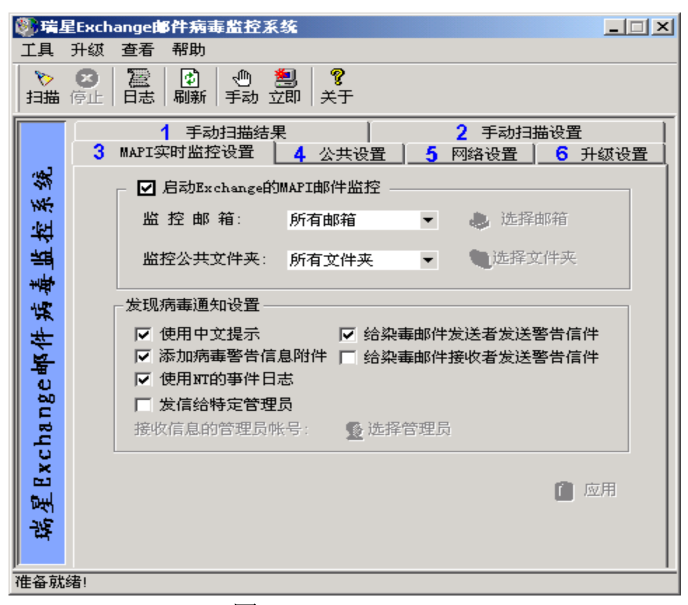


图 3-1

1. MAPI 邮件实时监控范围设置

此项功能是使用 MAPI 接口，对用户邮箱和公用文件夹中新到的邮件进行实时监控，一旦有新邮件到达时，程序自动对邮件进行扫描。此项设置根据对象具体可以分为两种，一种是监控邮箱，一种是监控公共文件夹，如图 3-2。

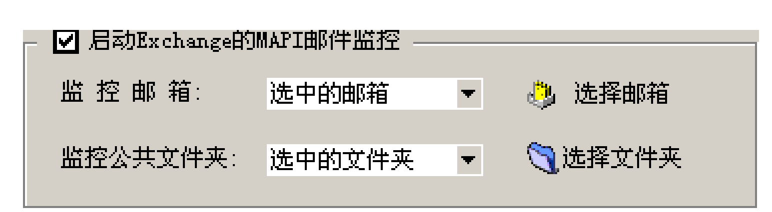


图 3-2

监控邮箱：选择需要进行监控的邮箱。其中有三项选择：所有邮箱、选中的邮箱和不监控邮箱。如果选择“选中的邮箱”项，需要单击右边的“选择邮箱”按钮，选择要监控的邮箱，如图 3-3。

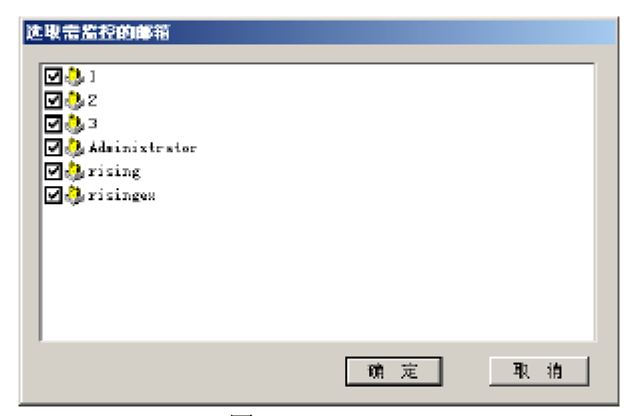


图 3-3

监控公共文件夹：选择需要进行监控的公共文件夹。操作过程和监控邮箱设置一样。

2. 发现病毒通知设置

功能：在实时监控和扫描病毒的过程中，如果发现病毒后，系统所采取的警告信息方式，如图 3-4。

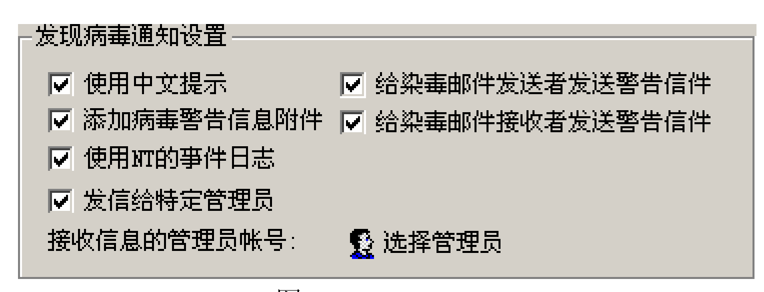


图 3-4

使用中文提示：扫描后在扫描结果里显示中文，否则，显示英文。

添加病毒警告信息附件：在邮件里添加一个纪录有病毒信息的文本文件。

使用 NT 的事件日志：把病毒信息纪录在 NT 的事件日治里。

给染毒邮件发送者发送警告信件：给邮件的发送者发送一封正文纪录病毒信息的邮件。

给染毒邮件接收者发送警告信件：给邮件的接收者发送一封正文纪录病毒信息的邮件。

发信给特定管理员：给特别指定的账号发送一封正文纪录病毒信息的邮件，单击右边的“选择管理员”按钮，选择账号即可。

二、公共设置

此项页签主要负责设置实时监控和扫描邮件时，查杀的文件类型、种类，以及查到病毒后的处理方式，如图 3-5。

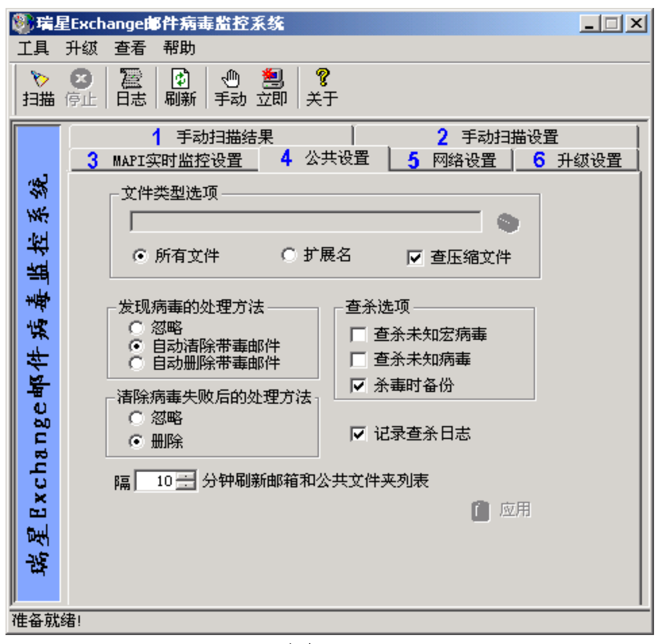


图 3-5

1. 查杀文件类型、查杀选项

1) 文件类型选项

功能：设置实时监控和手动扫描时的文件类型。可以选择查杀所有文件或者按扩展名查杀，当选择“扩展名”时，需要单击文本框右边的小按钮选择具体的文件类型，如图 3-6。

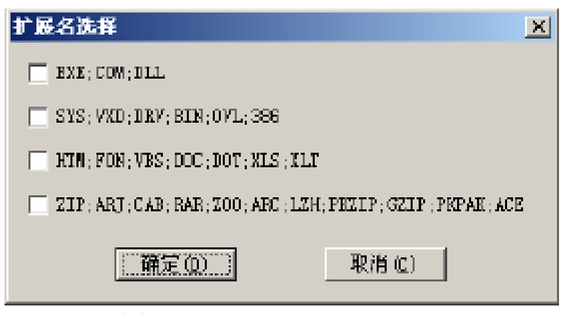


图 3-6

查杀同时可以复选是否查杀压缩文件。

2) 查杀选项

查未知宏病毒：选择后可检测出携带未知宏病毒的文件和带有宏的 Office 文件。

杀毒时备份：当您在查杀选项中选择了“杀毒时备份”，那么所有您清除或删除的染毒文件都会在“病毒隔离系统”中隔离起来，并可安全的恢复，避免设置或误操作造成的文件丢失损坏。

2. 发现病毒的的处理方式

1) 发现病毒的处理方法

忽略：不对病毒做任何处理，但把病毒信息记录在警告信息里。

自动清除：直接清除附件文件里的病毒，并把病毒信息记录在警告信息里。

自动删除：直接删除携带病毒的附件文件，并把病毒信息记录在警告信息里。

2) 清楚病毒失败后的处理方法

此项设置主要针对一些不能清除病毒的文件类型。

例如，压缩文件，现在版本不能直接清除或删除压缩文件里的病毒文件，软件在处理这些文件时就是清除失败，那么软件处理此类性文件时即按照此项设置处理。

忽略：不对病毒做任何处理，但把病毒信息记录在警告信息里。

删除：直接删除携带病毒的附件文件，并把病毒信息记录在警告信息里。

3. 其他设置

1) 日志

把手动扫描记录到文本文件。

2) 刷新邮箱和公共文件夹列表时间间隔

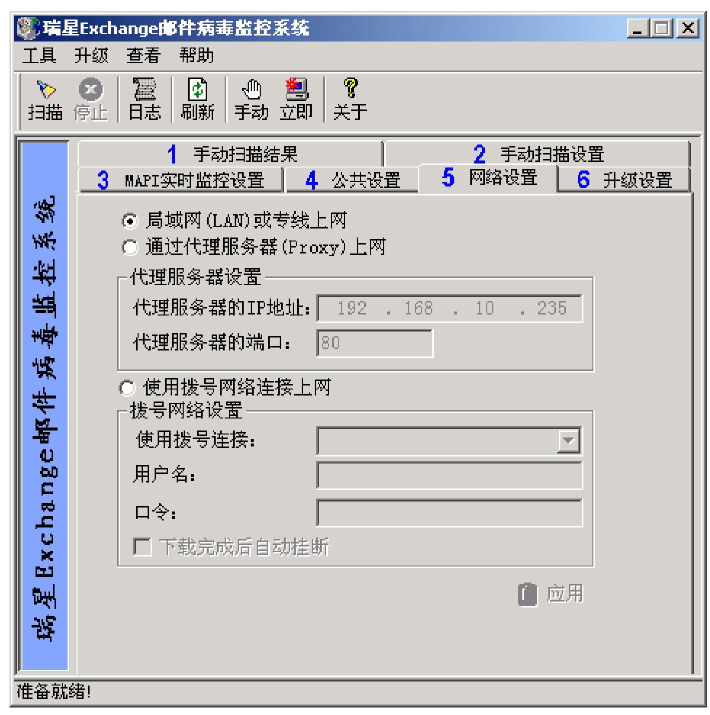
隔一定的时间刷新邮箱和公共文件夹，把新的邮箱和公共文件夹列入监控对象里。

三、网络设置

功能：在升级之前配置好您的局域网与瑞星网站连接。

1. 局域网（LAN）或专线上网

如果安装瑞星 EXCHANGE 邮件病毒监控系统的计算机使用直接连接 Internet 的方式上网的，就可以选择此项，如图 3-7。



3-7

2. 通过代理服务器（Proxy）上网

如果安装瑞星 EXCHANGE 邮件病毒监控系统的计算机是通过代理服务器上网，就可以选择该项，网络设置会自动读取计算机上的使用的代理服务器的 IP 地址及端口号，如图 3-8。

图 3-8

在启动“网络设置”时，如果软件读不出计算机上的使用的代理服务器的 IP 地址及端口号，则说明代理服务器设置不正确，可手工输入 IP 地址及端口号。

3. 使用拨号网络连接上网

如果安装瑞星 EXCHANGE 邮件病毒监控系统的计算机没有使用以上两种上网方式，而是以拨号连接上网方式的，启动“网络设置”时也会自动读取当前默认的拨号连接方式，如图 3-9。

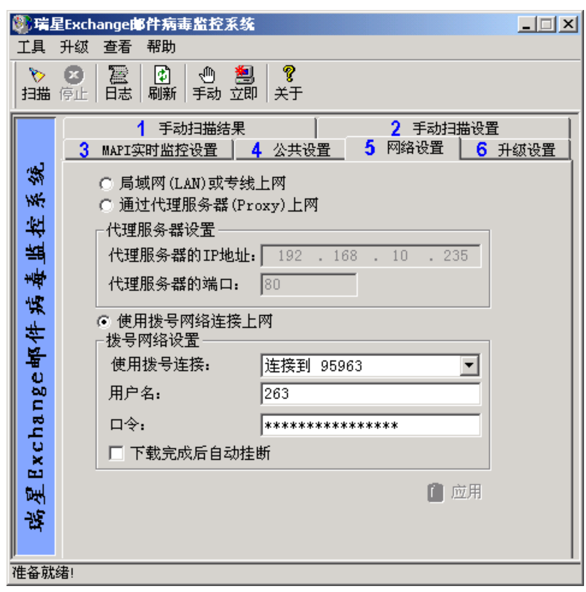


图 3-9

四、升级设置

升级是通过菜单栏中“立即”菜单命令，升级设置来设定在进行升级之前，必须选择的最适合、最简便的升级方式，瑞星公司提供了如下几种升级方式，如图 3-10。

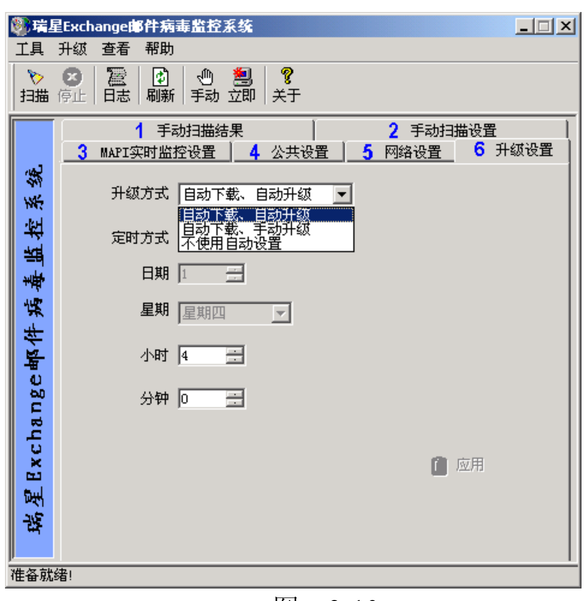


图 3-10

1. 自动下载、自动升级

对于网络连接方便，全自动化功能要求较高的用户建议采用这种方式，瑞瑞星 EXCHANGE 邮件病毒监控系统会设定好时间智能地升级。

2. 自动下载、手动升级

对于网络连接方便，但网络安全性要求较高的用户建议采用这种方式，自动下载升级程序后，可以先在试验网上验证无误或当前时机适合进行全网升级时进行手动升级。

3. 不使用自动设置

对于网络连接不方便或不能与 Internet 连接的用户建议采用这种方式。

定时方式：主要是设置自动升级时的时间。

五、手动扫描设置

选择手动扫描的邮箱和公共文件夹，如图 3-11。

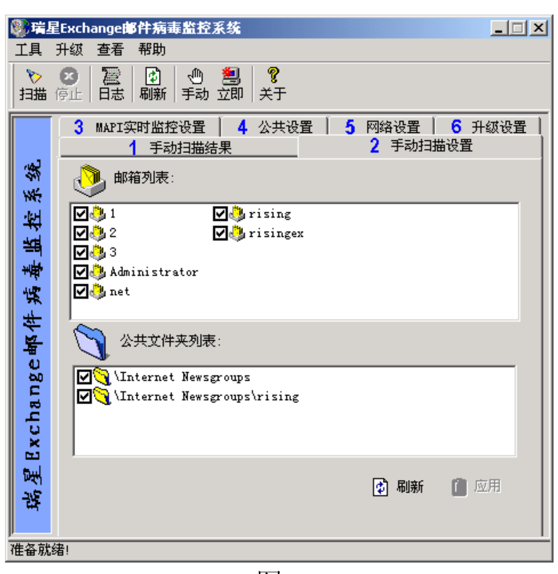


图 3-11

六、手动扫描结果

纪录手动扫描的结果：带病毒邮件名称、附件文件名称、病毒名称和处理方式，如

图 3-12。



图 3-12

七、菜单命令

1. 工具

扫描：手动扫描邮箱和公共文件夹。
停止：停止手动扫描。
查看日志：查看手动扫描的纪录。
退出：退出瑞星 EXCHANGE 邮件病毒监控系统主界面。

2. 升级

立即升级：升级命令。

3. 查看

刷新：刷新邮箱和公共文件夹。

➢ **注意事项：**每一项页签设置后，只有单击“应用”按钮后才能生效。

第四章 使用

本章主要介绍软件的具体应用方法、以及一些注意事项。

一、应用

1. 设置实时监控和公共设置选项。单击各项页签的应用按钮，使设置生效。
2. 设置完成后，在发送邮件的时候，实时监控已经开始检查邮件是否携带病毒。
3. 可以定期，或者根据需要，手动扫描邮箱检查邮件是否携带病毒。

二、升级

系统升级方法可以分为自动下载自动升级和自动下载手动升级两种。
具体如何设置升级方法参看功能部分。

1. 自动下载自动升级

   1) 设置“网络设置”。
   2) 单击立即按钮，开始连接瑞星网站。
   3) 连上瑞星网站后，关闭一些服务，从网站上下载需要升级的程序。
   4) 升级完成后，重启服务。

2. 自动下载、手动升级

   1) 设置“网络设置”。
   2) 单击立即按钮，开始连接瑞星网站。
   3) 连上瑞星网站后，从网站上下载升级包，升级包名称为 update.exe，存放路径为安装目录下的 ManualUpdate 目录下。
   4) 升级包下载完后，管理员单击“手动”按钮，选择下载的升级包，单击打开即可。

➢ 注意事项

1、在 Exchange 5.5 下，瑞星 Exchange 邮件监控系统采用基于 MAPI 方式的邮件监控和扫描，只能实时监控接收到的新邮件，不能监控发送的邮件。

2、在 Exchange 2000 下，除了采用与 Exchange 5.5 相同的 MAPI 监控方式外，新增加了基于 SMTP 的实时监控，不仅能对接收到的新邮件进行实时监控，也能够对发送的邮件进行监控。（当然前提条件是启用“SMTP 实时监控”）。在某些特定的条件下，这两种监控方式可能产生重叠，因而产生两个病毒警告附件或发送两个病毒警告邮件。

3、对于 MAPI 方式的实时监控，瑞星 Exchange 邮件监控系统在接收到“新邮件到达”的通知后，对邮件进行扫描。如果在扫描过程中，用户将邮件从服务器上移走，瑞星 Exchange 邮件监控系统将无法完成对邮件进行的修改。在这种情况下，瑞星 Exchange 邮件监控系统发送的病毒警告邮件中，将提示用户：邮件仍处于染毒状态。而对于 SMTP 实时监控，在瑞星 Exchange 邮件监控系统完成对邮件的操作之前，邮件不会被移走。

4、对于新建的邮箱，只要用户没有选择“不监控所有的邮箱”（也就是选择了“监控所有的邮箱”或者选择“监控指定的邮箱”），瑞星 Exchange 邮件监控系统将自动对新建的邮件进行保护。新建公用文件夹的监控与此类似。需要注意的是，该功能受刷新间隔的影响，缺省的刷新间隔是 10 分钟，用户可以根据实际情况对此值进行重新设置。刷新邮箱和公用文件夹列表是一件很费时和很耗资源的操作，如果邮箱和公用文件夹的总数比较多的话，应该增大刷新间隔，以减轻服务器的负荷。